DOCUMENT RESUME

ED 419 538 IR 057 040

AUTHOR Rosenblum, Cindy
TITLE E-Mail at Work: Is it Really Private?
PUB DATE 1997-12-00
NOTE 22p.; Paper submitted to the Annual Convention of the Broadcast Education Association (BEA) (43rd, Las Vegas, NV, April 3-6, 1998).
PUB TYPE Reports - Evaluative (142) -- Speeches/Meeting Papers (150)
EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS *Computer Mediated Communication; Court Litigation; *Electronic Mail; Employee Attitudes; *Employment Practices; *Information Policy; Laws; *Privacy; Work Attitudes; Work Environment

ABSTRACT

This paper examines the controversy of e-mail privacy in the workplace. Once an employee uses an e-mail system that belongs to the employer, according to recent case law, their privacy rights are forfeited. Employers will now have to start creating policies to safeguard themselves from expensive litigation, and employees will have to be more careful about what kind of messages they send over their employer's e-mail system so that they do not get fired. This controversy may change behavior of employees in the workplace dramatically. They may feel stifled if they have to watch the content of every e-mail message they send. However, it may be for their own good not to divulge any personal information or personal opinions over the company system. (AEF)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED 419 538

INDIANA UNIVERSITY
DEPARTMENT OF TELECOMMUNICATIONS
RADIO AND TELEVISION, #261
BLOOMINGTON, INDIANA 47405

E-MAIL AT WORK: IS IT REALLY PRIVATE?

A "DEBUT" PAPER SUBMITTED TO
THE LAW & POLICY DIVISION OF BEA
FOR THE 43RD ANNUAL CONVENTION:
"ELECTRONIC MEDIA AND SOCIETY:
ROLES AND RESPONSIBILITIES"

BY

CINDY ROSENBLUM

BLOOMINGTON, IN

DECEMBER 1997

IR057040

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION
CENTER (ERIC)
☐ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

PERMISSION TO REPRODUCE THIS
MATERIAL HAS BEEN GRANTED BY
Cindy Rosenblum
TO THE EDUCATIONAL RESOURCES
INFORMATION CENTER (ERIC)

Abstract

This paper examines the controversy of e-mail privacy in the workplace. Once an employee uses an e-mail system that belongs to the employer, do their privacy rights go out the window? According to recent case law, yes they do. Employers will now have to start creating policies to safeguard themselves from expensive litigation, and employees will have to be more careful about what kind of messages they send over their employee's e-mail system so that they do not get fired.

This controversy may change behavior of employees in the workplace dramatically. They may feel stifled if they have to watch the content of every e-mail message they send. However, it may be for their own good not to divulge any personal information or personal opinions over the company e-mail system.

Introduction

We are in an age now where computer technology is developing rapidly. Many businesses welcome the onset of new technology with open arms, embracing the opportunity to increase productivity. However, new computer technologies do not only effect the immediate goals of the business. They change traditional business practice and traditional behaviors in the office on a day-to-day basis as well. The technology that will be focused on in this paper is electronic mail that is used at the workplace.

Before e-mail was used in offices, if an employee received a letter in a sealed envelope, it was assumed by the employee that nobody else had read the letter except the sender. With e-mail used at the workplace, employees cannot safely assume that the messages they get will not be read by anyone else. Technically, the e-mail systems that they are using are owned by the company that they work for.

This paper will explore the controversy surrounding e-mail privacy in the workplace. According to the few recent court cases in this area, employers feel that they own the e-mail system, and therefore have every right to see what the employees are using e-mail for. The employees feel that if the employer specifies that their e-mail is private, they have an absolute right to e-mail privacy, and the courts are leaning toward

agreeing with the employers. This paper will discuss the recent litigation and some social implications of this controversy.

The Controversy: Employees v. Employers

Recent court cases have indicated that employees have no privacy rights when their e-mail is sent through the employer's system.

In *Bourke v. Nissan Motor Co.*[1], an e-mail message sent by Bourke to another employee was randomly selected to show a group of employees at an e-mail training session. Unfortunately for Bourke, the "e-mail was of a personal, sexual nature and not business-related."[2] This incident was reported to Bourke's supervisor, who

> with management's authorization reviewed the e-mail messages of the entire workgroup. Nissan found substantial numbers of personal, including sexual messages from Bourke . . . and issued written warnings to plaintiffs for violating the company policy prohibiting the use of the company computer system for personal purposes.[3]

Bourke was subsequently fired for what Nissan said was an "unsatisfactory" rating and she "sued Nissan for invasion of privacy."[4]

---

[1]*Bourke et al., v. Nissan Motor Corporation.*, No. B068705 (Cal. Ct. App. Jul. 26, 1993). (visited Nov. 13, 1997) <http://www.lexonline.com:80/bourke.htm>.

[2]*Id.* at 2.

[3]*Id.* at 2.

[4]*Id.* at 2.

The court said that Bourke had no reasonable expectation of privacy, and "In the absence of a reasonable expectation of privacy, there can be no violation of the right of privacy."[5]

The reasons why Bourke had "no reasonable expectation of privacy" was that Nissan had the following facts on its side:

> 1) Bourke signed a Computer User Registration Form, which states that "It is company policy that employees and contractors restrict their use of company-owned computer hardware and software to company business."
> 2) . . . Bourke learned from co-workers that e-mail messages were, from time to time, read by individuals other than the intended recipient.
> 3) A full six months before Bourke's termination, a fellow employee contacted Bourke to complain about the personal, sexual nature of Bourke's e-mail message which was retrieved for demonstration purposes during a training session at an Infiniti dealership.[6]

The outcome of this case spawned a controversy in the press. Kelly Payne, writing for *The Internet Law Handbook Newsletter*, said the following:

> In my opinion, this is simply a case of the law lagging behind technology. For instance, the company owns the phone system at your office, but it cannot tap your phone line. Similarly, your boss cannot pick up a letter on your desk addressed to you at work and delivered by the U.S. postal service and open and read it. Why should your e-mail be any different. It shouldn't.[7]

---

[5]*Id.* at 3.

[6]*Id.* at 4.

[7]Kelly Payne, *Privacy Rights in your E-Mail at your Workplace* [for the Internet Law Handbook Newsletter] (visited November 6,1997) <http://www.lexonline.com:80/emailprivacy.htm>.

What Ms. Payne is failing to address here is that e-mail and "snail-mail" are used in different ways. Sometimes, an employee will use e-mail to avoid confrontation with a supervisor if they do not want to talk to them face to face. This can be beneficial to both the employee and the employer.

> Workers can send messages at their convenience, without having to wait for an appointment or to catch the manager in the hall. It also can alleviate employee reluctance to talk. Workers feel less intimidated about talking to the boss electronically than they do about talking to him or her face-to-face, particularly if what the worker wants to say is in any way negative. Because there are few reminders of status differences, the fear of evaluation or criticism declines.[8]

Before e-mail, if an employee wanted to talk to a supervisor or another co-worker, it would simply be easier to walk over to his or her cubicle or office and talk in person. However, if the employee wanted to talk to a supervisor and was intimidated, he or she could always write a memo. If a memo is written, there is no guarantee that nobody else would see it unless it was in a sealed envelope. If the employee decided to ask in person, there was no guarantee that there would be privacy because somebody else could overhear the conversation. Memos, "snail-mail", and in-person confrontations were used for business purposes only, whereas e-mail is not only used for business.

---

[8]Lee Sproull and Sara Kiesler, *Increasing Personal Connections, in* COMPUTERIZATION AND CONTROVERSY: VALUE CONFLICTS AND SOCIAL CHOICES, 2ND ED. 455, 463 (Rob Kling ed., 1996).

The other major difference between e-mail and "snail-mail" is that within a corporate setting, if you send or receive a letter on paper that you don't want anyone to see, you can put it through the paper shredder. With e-mail, it is quite different. Even if the sender or receiver of a message uses the "delete" feature, the messages are still stored in a database.

Employees are also under the impression that since e-mail is in an electronic medium and they have "secure" passwords, that it is private.

> Bourke asserts that she had a 'reasonable expectation of privacy' because they were given passwords to access the computer system and were told to safeguard their passwords.[9]

Bourke did not have a 'reasonable expectation of privacy because the company owned the computers and e-mail system.

> . . . one commentator has suggested that "because most systems generally limit access to those who provide personal passwords or numbers, many employees will have a subjective expectation of privacy in their use of the system, notwithstanding the fact that the computer is owned by the company."[10]

Additionally, employees still tend to write personal messages to each other (what are you doing for lunch today?) even though some employers specify that e-mail is strictly for

---

[9] *See supra* note 1, p. 4.

[10] Donald H. Seifman and Craig W. Trepanier, E-mail and Voicemail Systems. Evolution of the Paperless Office: Legal Issues Arising out of Technology in the Workplace, part 1, Employee Relations Law Journal, 5, 7 (December 22, 1995).

business use. "Snail-mail" and memos would not be used in this case. The methods now for talking to co-workers while appearing to "look busy" is to e-mail them. It is certainly more "official looking" than making a phone call to another office or cubicle, and nobody else can "hear" what you are actually saying, unless someone is looking over your shoulder and reading the screen.

E-mail at the workplace also brings out another use that would not be previously used in memos or traditional mail to protect the anonymity of the sender--using e-mail to harass co-workers. Karen L. Casser outlines this problem for employers in her article *Employers, Employees, E-mail and The Internet*:

> Unlike comments made in public around a water cooler, an e-mail harasser or stalker can conduct his activities privately. Unless the recipient discloses the harassment, it can continue unnoticed. E-mail facilitates effortless communications and redistribution to large groups of people multiplying the damages. . . . Knowledge of these types of messages should be taken seriously and treated as any other suspected harassment and investigated immediately.[11]

Employers can tell their employees that their e-mail will be private, but it still might not be so, as shown by what Epson America did with Alana Shoars. Shoars was hired by Epson to "provide training and user support for software use, emphasizing

---

[11]Karen L. Casser, *Employers, Employees, E-mail and The Internet in* THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES (visited Nov. 6, 1997) <http://cla.org/RuhBook/chp6.htm>.

Epson's e-mail system."[12]

> Employees accessed the e-mail using personal passwords, and Shoars had informed them their e-mail was private and confidential.[13]

Shoars saw her supervisor printing out and reading e-mail messages from the employees of the company. She insisted that he stop, and was threatened with her job. Shoars reported her supervisor for reading the e-mail, and he subsequently fired her, "under the pretext she had been insubordinate in asking Epson's e-mail manager to provide her a personal outside e-mail line that the supervisor could not access."[14]

Shoars' supervisor "declared that he worked with the message file to assist users with problems they reported; in doing so, he printed out and flipped through copies of the messages, to find and read those with which problems were being experienced."[15] The court took the position that the supervisor or Epson did not violate any penal codes because they do not cover e-mail transmission. Additionally, the court said that "'downloading' of messages into storage by Epson's computer software did not

---

[12]*Alana Shoars v. Epson America, Inc.*, No. B073234 (Cal. Ct. App. April 14, 1994) (visited Nov. 6, 1997) <http://www.lexonline.com:80/shoars.htm>.

[13]*Id.* at 1.

[14]*Id.* at 1.

[15]*Id.* at 3.

constitute reading them or attempting to learn their contents."[16]

Kelly Payne also had a comment about this case:

> In an even more absurd case, a company employee was told to tell all company employees that e-mail was confidential. She later determined that her own e-mail had been read. She complained and was fired. She sued under the California anti-wiretapping statute, and a California court dismissed her case. Did this employee have a reasonable expectation of privacy? Clearly so. Yet the courts did not protect her "confidential" e-mails.[17]

Shoars may have had a reasonable expectation of privacy under what Epson had told her, but there was no written policy and she had apparently been misled by the company. Employees have no reasonable expectation of privacy if the company owns the system. Employers are interested in the efficiency of their employees. What is to stop an employer from looking through e-mail messages to see if the system is being strictly used for business?

> Legal experts, however, say this case could damage Epson significantly--to the tune of millions of dollars--because the company made one major error: It apparently misled Shoars about company policy although she was responsible for administering it. In addition, Shoars, by most accounts, had an exemplary record.[18]

Companies will run into problems unless they outline a policy telling employees exactly what the purpose of the e-mail

---

[16]*Id.* at 3.

[17]*See supra* note 7, p. 1.

[18]Robert Kane, *Can The E-Mail Envelope Be Digitally Steamed Open?* (visited Nov. 15, 1997) <http://www.intrusion.com/digital.htm>

system is. One company, Bankers Trust, has a policy so that there are no misconceptions of what their e-mail use is for.

> The Bankers Trust "Internet Communications Policy," published in October 1996, doesn't mince words. Each employee who gets connected must review and agree to the six-page policy. A section entitled "No Privacy and Monitoring" warns that management monitors all Internet communications, and that employees should not expect their e-mail to be private.[19]

To examine what corporate organizations were doing about the implementation of e-mail policies that gave employees privacy, the Society for Human Resource Management conducted a survey. "The survey drew from a random sampling of 3,000 members, with more than 500 responding."[20]

> The SHRM survey found that just under 40% of the organizations that use E-mail have implemented written E-mail privacy policies. While this isn't as high as we'd like to see, it's a remarkable figure in light of the relatively short time that e-mail has actually been deployed in the workplace.[21]

Some believe that the laws should be upgraded to reflect the new technology.

> . . . some courts have not kept up with technology. In two landmark cases, California courts sided with employers who had intercepted employee e-mails. The reasoning? The employees did not have a reasonable expectation of privacy, the courts ruled, although it is hard to believe the rulings would have been the same had the technology been a telephone

---

[19]Mary J. Cronin, *Tough Rules for Web Access*, FORTUNE, Aug. 4,1997, at 218.

[20]Michael F. Cavanaugh, *E-Mail Privacy: A Glass Almost Half-Full*, COMPUTERWORLD, March 18, 1996, at 37.

[21]*Id.* at 37.

> instead of an e-mail system. One court reasoned that since the business owned the e-mail system, it was entitled to see what was on it. Of course, that same business also owns its phone system, but wiretapping and other laws prevent eavesdropping in many cases.[22]

In another case, *Michael A. Smyth v. The Pillsbury Company,*[23] an employee who was reassured by the company that "all e-mail would remain confidential and privileged"[24] and " . . . that e-mail communications could not be intercepted and used by the company against its employees as grounds for termination or reprimand."[25]

Contrary to these assurances of confidentiality, Pillsbury intercepted Smyth's private e-mail messages. He was fired "for transmitting what the company deemed to be inappropriate and unprofessional comments over the company's e-mail system."[26] ("The e-mails concerned sales management and contained threats to 'kill the backstabbing bastards' and referred to the planned Holiday party as the 'Jim Jones Koolaid affair.'"[27])

---

[22]Sean Silverthome, *Who Owns Your Workplace E-Mail?* (visited Nov. 15, 1997) <http://www.thesite.com/0197w4/work/work379_012197.html>.

[23]914 F. Supp. 97; 1996 U.S. Dist. LEXIS 776; (visited Nov. 6, 1997) <http://epic.org/privacy/internet.smyth_v_pillsbury.html>.

[24]*Id.* at 1.

[25]*Id.* at 1.

[26]*Id.* at 1.

[27]*Id.* at 3.

The court

> did not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once Smyth communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.[28]

Michael Smyth tried to use the "intrusion upon seclusion" tort as his defense, which is as follows:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[29]

This defense did not work. The court said:

> . . . even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. By intercepting such communications, the company is not . . . requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.[30]

According to the outcome of this case, even though Michael Smyth was assured confidentiality in his e-mail, the court once

---

[28] *Id.* at 3.

[29] Restatement (Second) of Torts @ 652B.

[30] *See supra* note 23, p. 3.

again took the position that the employer has the right to monitor the content of the messages. Kevin G. DeNoce comments:

> First, private e-mail -- sent from and received at individuals' home addresses -- is protected under the privacy laws. Second, business e-mail -- sent from or received at an employer's address -- is not. In other words, employers can read messages sent or received via their companies' computer systems without violating employee's privacy rights.
>
> In cases in which employers lead employees to believe that e-mail messages will not be monitored -- for example, by stating so in company policy -- a good argument can be made that such communications are entitled to privacy. The degree of protection under the privacy laws, however, varies from state to state, and thus far, cases addressing the privacy of business e-mail have not found such communications to be protected.[31]

One commentator thought that the court did not look at the Smyth case in the way that it should have:

> The court never spells out the circumstances under which Smyth's mail came to Pillsbury's attention. . . .
>
> Reading the decision, you get the sense that the judges were not too familiar with e-mail; the excerpt quoted above seems to state that no-one should have any expectation of privacy in mail sent via a system "utilized by the entire company." This, of course, is tantamount to saying that you shouldn't assume the privacy of mail sent U.S. post, because the postal service is used by everyone.[32]

In addition to the cases already noted, in *Thomasson v. Bank of America*,[33] an "employee was fired after the employer

---

[31]Kevin G. DeNoce, *Internet Privacy Jurisprudence Begins to Develop*, NATIONAL LAW JOURNAL, B11 (July 21, 1997).

[32]Jonathan Wallace, *EMAIL PRIVACY: What are your rights?* (visited Nov. 15, 1997) <http://www.pencom.com/law/email.html>.

[33]1995 Cal. LEXIS 1843, March 15, 1995, *appeal denied* by Supreme Court of California.

discovered e-mail messages which revealed that the employee worked as a professional gay stripper."[34]

From examining these cases, the consensus among the courts seems to be that employees should not expect that any message they send will be private at all. Since there are already laws in place for tapping phone lines and looking through U.S. Mail, until there is a set of specific laws regarding e-mail, employees should keep their guard up when sending messages.

> "Employees are under the misapprehension that the First Amendment applies in the workplace and it doesn't," said Neal J. Friedman, a Washington attorney who specializes in on-line law. "Employees need to know they have no right of privacy and no right of free speech using company resources."[35]

Implications of the Debate

With all of this litigation going on regarding the privacy of employee e-mail, there are different social implications that are raised. This section will outline the social aspects of having e-mail at work and how the court's actions may affect employee behavior.

Employees feel that if there is an e-mail system at work and if they have a secure password, they should be able to assume that their messages will be private. Employers feel that since they own the system, even if they promise the employees that

---

[34]*See Supra* note 11, p. 9.

[35]Mitch Wagner, *Firms Spell Out Appropriate Use of Internet for Employees*, COMPUTERWORLD, Feb. 5, 1996, at 55.

their e-mail will be confidential, they can still monitor the e-mail messages. The courts are ruling in favor of the employers.

This could completely change how people interact with each other in the workplace. Instead of welcoming e-mail as a convenient way to conduct business with co-workers, employees might become afraid to even send that e-mail message that says "what are you doing for lunch?" It has the potential to create a different work atmosphere where people have to really think about every message that they send. Corey L. Nelson writes:

> A rigid office will produce only oppressed workers with little incentive to go that extra mile when the company needs it. Productivity does not flourish in a hostile workplace. A Big Brother attitude only squelches creativity, something on which American industry was built and on which it very much depends to compete in global markets. If a company desires contented, productive and long-term employees, it must recognize their right to privacy.[36]

She also feels that if there is no e-mail privacy at work, it will soon lead to other violations of privacy.

> If an employer claims to have the right to monitor E-mail at its discretion (to whatever intangible degree that might be), then how long before it listens to our private calls, reads our mail or plants a microphone by the water cooler? Wireless telephones are legally required to have written notices stating that communications aren't private. Where are the E-mail privacy warnings?[37]

While this view might be a bit extreme, there is some

---

[36]Corey L. Nelson, *IS E-MAIL PRIVATE OR PUBLIC? Employers Have No Right to Snoop Through Mail*, COMPUTERWORLD, June 27, 1994, at 135.

[37]*Id.* at 135.

evidence that privacy in the workplace in general is at a minimum. In the Society for Human Resource Management survey mentioned previously, "less than one-third of all SHRM respondents reported having any privacy policies about access to desk drawers, file cabinets and lockers, for example."[38]

> Why are there more policies governing E-mail than ones governing a worker's desk? "Privacy policies are equally important for paper-based information as they are for digital information, but it appears that E-mail provides the impetus for many organizations to get a grip on privacy issues," observes SHRM President and CEO Michael R. Losey.[39]

There is also the other extreme. Some employees might not even care about their e-mail or might not even use it. Additionally, some might even feel that their employer doesn't want to waste the time or energy going through all of the employee e-mail. However, if they do feel this way, they should still exercise caution in the messages they send, just in case they are caught sending an inappropriate message.

Finally, e-mail does have some social benefits for employees in the workplace, aside from the privacy issue. Employees who are lower on the totem pole might not have access to or might not care about the information that they need. "Electronic communication may offer peripheral employees new opportunities to initiate connections within the organization to reduce the

---

[38] *See supra* note 20, p. 37.

[39] *Id.* at 37.

information gap and increase motivation."[40] Additionally, "receiving mail can affect employees' attitudes toward their organization by increasing their informational and emotional connections to other employees."[41] People may be conversing over e-mail with other employees that they would never be able to without it. "Reading messages gives employees the opportunity to make connections with other employees who would otherwise be invisible or unknown."[42]

Although privacy rights concerning e-mail are a controversial issue, the benefits of employee use of e-mail should not be overlooked.

Summary & Conclusion

E-mail at the workplace has the potential to change employee behavior dramatically. Employees use e-mail differently than regular U.S. mail or "snail-mail" and paper memos. Privacy of paper letters and memos was safely assumed. If a worker wanted to get rid of a letter that he or she received, they would just put it through the shredder. With the increasing use of e-mail at work, employees are learning that just using the "delete" feature and having secret passwords isn't enough to secure their privacy.

---

[40] *See supra* note 8, p. 456.

[41] *Id.* at 457.

[42] *Id.* at 459.

Additionally, the courts feel that employees do not have any reasonable expectation of privacy when using an e-mail system that belongs to the company. This has caused employers to seek legal advice concerning the creation of e-mail privacy (or non-privacy) policies for their employees. It also may lead to employees having to write every e-mail message with caution.

Unfortunately, some employees use e-mail to sexually harass other employees, which (in my view) might justify the employer periodically checking out the e-mail. However, if this becomes the case, employees should remember that e-mail at work is not a free forum. Employees cannot curse out their boss and other supervisors like Michael Smyth did, or send e-mails of a personal and sexual nature like Bonita Bourke did. They also should not reveal personal secrets as the worker who was moonlighting as a gay stripper did in *Thomasson v. Bank of America*.[43]

Employers should get into the habit of having and maintaining e-mail policies that employees can readily understand. Bank of America leaves no question in their employee's minds that their e-mail is monitored.

As with anything else in the workplace, employees should understand that it is best when you leave your personal feelings at home when you are on the job. However, this is very difficult in an electronic forum. Anonymity is easy to have, and it is

---

[43]*See supra* note 33.

easier to confront people that employees wouldn't even talk to under any other circumstances.

However, the courts keep ruling in favor of the employer because there really is no legislation regarding e-mail. There are already laws against wiretapping, so laws against monitoring e-mail may not be far behind.

Behaviors might change at the workplace if the surveillance of e-mail continues. Employees may feel that the work atmosphere is very rigid if they cannot freely use their e-mail without having a third party read it. However, some employees may feel that they have nothing to hide in their e-mail and if they aren't doing anything wrong, it is not a big deal for someone else to look at it.

Whatever the outcome, it appears that the trend will be for employers to begin the implementation of e-mail policies for their employees. Due to the recent case law in this area, they have no other option. They will avoid expensive litigation if they do so. Additionally, employees will have to be more careful of what they are sending over their employer's e-mail system. To some people, having e-mail at work is a "toy," and workers will play with it either to look busy or to send notes to their friend in the cubicle next to them about the guy in the adjacent office. However, employees will have to learn that e-mail is not a toy, and that it can be used against them if they are caught sending

messages that aren't business related.